COLLOQUIUM MATHEMATICUM

VOL. 84/85 2000 PART 1

DYNAMICAL SYSTEMS ARISING FROM ELLIPTIC CURVES

BY

P. D'AMBROS, G. EVEREST, R. MILES AND T. WARD (NORWICH)

Dedicated to the memory of Professor Anzelm Iwanik

Abstract. We exhibit a family of dynamical systems arising from rational points on elliptic curves in an attempt to mimic the familiar toral automorphisms. At the non-archimedean primes, a continuous map is constructed on the local elliptic curve whose topological entropy is given by the local canonical height. Also, a precise formula for the periodic points is given. There follows a discussion of how these local results may be glued together to give a map on the adelic curve. We are able to give a map whose entropy is the global canonical height and whose periodic points are counted asymptotically by the real division polynomial (although the archimedean component of the map is artificial). Finally, we set out a precise conjecture about the existence of elliptic dynamical systems and discuss a possible connection with mathematical physics.

Introduction. Let $F \in \mathbb{Z}[x]$ denote a primitive polynomial with degree d, which factorizes as $F(x)=b\prod_i(x-\alpha_i)$. Then F induces a homeomorphism T_F on a compact, d-dimensional group $X = X_F$, via the companion matrix of F. The group X is a *solenoid* whose definition is discussed in Section 2 below. The essential properties of this dynamical system $T_F : X \to X$ are as follows.

1. The topological entropy $h(T_F)$ is equal to

$$m(F) = \int_0^1 \log|F(e^{2\pi it})|\,dt = \log|b| + \sum_{i=1}^{d} \log^+|\alpha_i|, \tag{1}$$

the Mahler measure of F.

2. Let $\mathrm{Per}_n(F)$ denote the subgroup of X consisting of elements of period n under T_F, i.e. $\mathrm{Per}_n(T_F)=\{x \in X : T_F^n(x) = x\}$. If no α_i is a root of unity,

2000 *Mathematics Subject Classification*: 37C35, 11G07.

The first author gratefully acknowledges the support of INdAM, the third of EPSRC grant 97700813, and we thank the anonymous referee for careful comments which have improved the exposition.

then $\mathrm{Per}_n(T_F)$ is finite with order

$$|\mathrm{Per}_n(T_F)| = |b|^n \prod_i |\alpha_i^n - 1|. \tag{2}$$

For background, and proofs of these statements, see [6, II] and [15]. When F is monic with constant coefficient ± 1 then X is the d-torus $\mathbb{T}^d$ and T_F is the automorphism of the torus determined by the companion matrix to F. The immanence of the circle is seen in both 1 and 2 above: the Mahler measure is the logarithmic integral of $|F|$ over the circle, and the periodic points formula is equivalent to evaluating the nth division polynomial of the circle on the zeros of F. That is, if we take $\phi_n(x) = \prod_{\zeta^n=1}(x-\zeta)$, we get the formula $\alpha^n - 1 = \phi_n(\alpha)$, so $|\mathrm{Per}_n(T_F)| = |b^n \times \prod_i \phi_n(\alpha_i)|$.

Both the Mahler measure and the nth division polynomial on the circle have natural analogues on elliptic curves, and our purpose here is to discuss a family of dynamical systems whose immanent group is an elliptic curve defined over the rationals. Assuming $d = 1$ for example, we hope for such a dynamical system with the single zero of F corresponding to the x-coordinate of a rational point on that curve. In other words, for every elliptic curve E and every point $Q \in E(\mathbb{Q})$ we are seeking a continuous map $T = T_Q : X \to X$ on some compact space $X = X(E)$ whose dynamical data should be described by well-known quantities associated with the point on the curve. We expect the entropy of T to be the global canonical height of the point Q (a well-known analogue of Mahler's measure) and the elements of period n should be related to the elliptic nth division polynomial evaluated at the point Q.

There now follows a brief description of this paper, explaining where to look for our main conclusions. For reasons we will present in Sections 2 and 3, it is to be expected that the underlying space X should be the adelic curve. Section 2 recalls the classical definition of the solenoid and the action F induces on it. Lind and Ward [10] reworked the classical theory in adelic terms, showing that the topological entropy can be decomposed into a sum of local factors, each of which is the entropy of a corresponding local action. Each of these local factors can be identified as a corresponding local component of the Mahler measure. Section 3 recalls the basic theory of elliptic curves needed; in particular, the decomposition of the global canonical height into a sum of local factors. Also, we recall that the p-adic curve is isomorphic to a simpler group, on which we may expect to define dynamical systems. In Section 4, in particular the conclusion, we will construct a dynamical system where the underlying space is a p-adic elliptic curve and where the map is induced by a point on that curve. The map in question is a p-adic analogue of the well-known β-transformation. The entropy of the map is the local canonical height of the point, and the periodic points can be counted

exactly. In Section 5, we consider how to glue together these local maps to get a global dynamical system. Here we are given an elliptic curve E defined over $\mathbb{Q}$ and a rational point $Q \in E(\mathbb{Q})$. The point Q induces a dynamical system where the underlying space is the elliptic adeles and the entropy turns out to be the global canonical height of the point Q. The construction of the map at the archimedean prime is artificial since it relies upon *a priori* knowledge of the height of the point (although it is a curious coincidence that the map is a classical β-transformation). We hope this will bring into better focus the construction at the non-archimedean primes where the map uses no such *a priori* knowledge of the height. The artificiality of the map is somewhat redeemed when we go on to show that the periodic points are counted asymptotically by the real division polynomial at the point Q. This last result makes use of some non-trivial results: one from elliptic transcendence theory and the other a result about periodic points for the classical β-transformation. Finally, in Section 6, we make some remarks about putative elliptic dynamical systems with the precise periodic point behaviour and discuss possible connections with mathematical physics.

2. The solenoid. Given $F(x) = bx - a$, with $a, b \in \mathbb{Z}$ coprime, let X_F denote the subgroup of $\mathbb{T}^{\mathbb{Z}}$ defined by

$$X_F = \{\mathbf{x} = (x_k) : bx_{k+1} = ax_k \text{ for all } k \in \mathbb{Z}\}.$$

The group $\mathbb{T}^{\mathbb{Z}}$ is compact by Tikhonov's theorem, and X_F is a closed subgroup so it too is compact, an example of a (1-dimensional) *solenoid*. More generally, a solenoid is any compact, connected, abelian group with finite topological dimension (see [8]). The automorphism T_F is defined by the left shift-action

$$T_F(\mathbf{x})_k = x_{k+1}. \tag{3}$$

EXAMPLE 2.1. Take $b = 1$ and $a = 2$, so $F(x) = x - 2$. Then the group X_F is given by $\{\mathbf{x} = (x_k) : x_{k+1} = 2x_k\}$. This is a closed subgroup of $\mathbb{T}^{\mathbb{Z}}$, so the topological dual group of X_F is given by the quotient

$$\widehat{\mathbb{T}^{\mathbb{Z}}}/X^{\perp} \cong \mathbb{Z}[t^{\pm 1}]/(t-2)\mathbb{Z}[t^{\pm 1}] \cong \mathbb{Z}[1/2].$$

The dual map to the shift T_F is the automorphism $x \mapsto 2x$. Indeed, the construction of X_F from F gives the natural invertible extension of the circle doubling map. It is easy to see that T_F has $2^n - 1$ points of period n (since these points are found by solving the simultaneous equations $x_{k+1} = 2x_k$ and $x_{k+n} = x_k$ for all k on $\mathbb{T}$), and has topological entropy $\log 2$. Moreover, there is an isomorphism $\mathbb{R} \times \mathbb{Q}_2 \to \mathbb{R} \times \mathbb{Q}_2$ sending the discrete (diagonally embedded) subgroup $\mathbb{Z}[1/2]$ to its own annihilator, so there is a natural onto homomorphism $\mathbb{R} \times \mathbb{Q}_2 \to X_F$, which realizes the map T_F as a factor of the map $(x, y) \mapsto (2x, 2y)$.

In general, the map T_F defined at (3) has the properties 1 and 2 of Section 1 by [15] (see also [6] for a more elementary discussion). In other words,

$$h(T_F) = \log \max\{|a|, |b|\} = m(bx - a) = m(F)$$

(a form of Abramov's formula). Our assumption on the zero of F not being a unit root amounts to $a \neq \pm b$, and the periodic points are given by

$$|\mathrm{Per}_n(T)| = |b|^n |\phi_n(a/b)| = |b^n - a^n|. \tag{4}$$

At the end of this section, we will show how the periodic points formula (4) comes about.

In order to motivate the name, and what follows, we now give a second equivalent definition of the solenoid and the action of T_F upon it. Define X to be the topological dual of the ring $\mathbb{Z}[1/(ab)]$. Then define T to be the map dual to $x \mapsto (a/b)x$ on $\mathbb{Z}[1/(ab)]$. The adelic point of view arises because X is isomorphic to the quotient of $\mathbb{R} \times \prod_{p|ab} \mathbb{Q}_p$ by the diagonally embedded discrete subgroup $\mathbb{Z}[1/(ab)]$ (this is a simple finite version of the standard adelic construction of the dual of an $\mathbb{A}$-field; see [3, Sec. 3] or [25, IV]). Each character on $\mathbb{R}$ restricts to a character on $\mathbb{Z}[1/(ab)]$; this induces a map from $\mathbb{R} \cong \widehat{\mathbb{R}}$ into X (injective since $\mathbb{Z}[1/(ab)]$ is dense in $\mathbb{R}$). The fact that the real line is "wrapped" densely into the compact group X accounts for the name solenoid. The group X is a semi-direct product of $\mathbb{T}$ by $\prod_{p|ab} \mathbb{Z}_p$. The action does not preserve the various local components, but a direct calculation of the entropy formula is possible (see [24]). Lind and Ward simplified this by working with the adeles proper, which live as a covering space to the one above. In that context, the map on each component is simply multiplication by a/b. Their approach involves tensoring the dual of X with $\mathbb{Q}$ which gives quick access to the standard results on adeles but destroys any periodic point behaviour (see [10, Sec. 3]). The elliptic system in Section 5 has the elliptic adeles as the base group, and for the finite primes, the local map is the local β-transformation by a/b. Thus it resembles the systems defined on both the solenoid and its adelic cover.

Finally, we examine how the periodic points formula (4) comes about. This will be instructive in Section 6, when we consider a possible elliptic analogue. The points of X_F having period n under T_F correspond to periodic vectors $\mathbf{y}$ of length n. The linear equation generated by such a vector is of the form $C\mathbf{y} = \mathbf{0}$, where C is the $n \times n$ circulant matrix on the row $(a, -b, \ldots)$. The number of solutions $\mathbf{y} \in \mathbb{T}^n$ of this equation, and hence the number of periodic points, is easily verified (see [6, Lemma 2.3]) to be $|\det(C)|$. From the well-known properties of circulants, this is equal to $|a^n - b^n| = |b^n \phi_n(a/b)|$.

3. Elliptic curves. In this section we recall some basic results about elliptic curves and fix the notation. A good account of elliptic curves can be

found in [16] and [18]; all that follows in this section can be found in those two volumes.

Denote by E an elliptic curve defined over a field K, and by $E(K)$ the group of points of E having co-ordinates in K. When $K = \mathbb{Q}$, Mordell's theorem says that $E(\mathbb{Q})$ is finitely generated and the torsion-free rank is referred to simply as the *rank*. Denote by $\widehat{h} : E(\mathbb{Q}) \to \mathbb{R}$ the global canonical height on $E(\mathbb{Q})$, a well-known analogue of Mahler's measure (see (1)). Denote by λ_p the local canonical height relative to the p-adic valuation. The formula that follows gives an important decomposition of the global height as a sum of local heights (see [16, Th. 18.2]):

$$\widehat{h}(Q) = \sum_{p \le \infty} \lambda_p(Q) \quad \text{for } Q \in E(\mathbb{Q}). \tag{5}$$

For finite p, whenever Q has good reduction at p,

$$\lambda_p(Q) = \tfrac{1}{2} \log \max\{|x(Q)|_p, 1\}. \tag{6}$$

Here and below, we refer to a rational point Q on E as having *good reduction* (respectively *bad reduction*) at a prime p if the image of the point under reduction modulo p is a non-singular (respectively singular) point on the reduced curve. In general, the local height is only defined up to the addition of a constant. The definition (6) agrees with the one in [17]. In [16], each local height is normalized by adding a constant to make it isomorphism-invariant. Whether normalized or not, (5) still holds.

If $K = \mathbb{R}$, the curve $E(\mathbb{R})$ is isomorphic to either $\mathbb{T}$ or $C_2 \times \mathbb{T}$ (see [18, V, Cor. 2.3.1]). Denote by $E_1(\mathbb{R})$ the connected component of the identity, which is always isomorphic to $\mathbb{T}$. If $K = \mathbb{Q}_p$, the curve $E(\mathbb{Q}_p)$ can be reduced modulo p. The set of points having good reduction is denoted by $E_0(\mathbb{Q}_p)$ and the kernel of the reduction is denoted by $E_1(\mathbb{Q}_p)$. For odd primes p, there is an isomorphism $E_1(\mathbb{Q}_p) \xrightarrow{\sim} p\mathbb{Z}_p$ (see [16, IV, Th. 6.4; VII, Prop. 2.2]). This isomorphism is essentially a logarithm and it comes from the theory of formal groups. The situation when $p = 2$ is similar; for details, see [16, IV].

These isomorphisms are analogous to the one from $E_1(\mathbb{R})$ to $\mathbb{T}$. The local isomorphisms for all primes p play a very important role in the development of dynamical systems because they allow actions on the additive local curves to be transported to the local curves proper. Consider the analogous situation in Section 1, where the immanent group is the circle. There is an isomorphism (the logarithm) from the circle to the additive group $[0, 1)$. The action on the circle really arises from an action on $[0, 1)$ which is then lifted via the logarithm to the circle itself. In the elliptic case, the local curve is isomorphic (via the elliptic logarithm) to an additive group. Subsequently, when we define an action on the p-adic curve, it will be one that is lifted from the additive curve. Thus, the dynamical systems which arise when the

immanent group is the elliptic curve are exactly analogous to the case where the immanent group is the circle (or more generally, the solenoid).

Finally, we recall the elliptic analogue of the division polynomial $x^n - 1$ on the circle. If E denotes an elliptic curve defined over $\mathbb{Q}$ then without loss of generality it is defined by a generalized Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with integral coefficients. There is a polynomial $\psi_n(x)$ with integer coefficients having degree $n^2 - 1$ and leading coefficient n^2 whose zeros are precisely the x co-ordinates of the points of E having order dividing n; for details see [18, Ex. 6.4, p. 477]. Later, we will consider the monic polynomial $\nu_n(x)$ of degree $n-1$ whose zeros are the x co-ordinates of the non-identity points in $E_1(\mathbb{R})$ having order dividing n,

$$\nu_n(x) = \prod_{\substack{nQ=O \\ O\neq Q\in E_1(\mathbb{R})}} (x - x(Q)). \tag{7}$$

The coefficients of $\nu_n(x)$ are real algebraic numbers, and for $Q \in E(\mathbb{Q})$, $\frac{1}{n}\log|\nu_n(x(Q))|$ converges to $\lambda_\infty(Q)$ (see [6, Th. 6.24]).

4. The β-transformation and a p-adic analogue. A comprehensive introduction to ergodic theory can be found in [21]. Here we just recall the definitions of ergodicity and entropy before examining in more detail the β-transformation and introducing its p-adic analogue. Let $T : X \to X$ be a measure-preserving transformation on the probability space (X, μ). Then T is *ergodic* if the only almost-everywhere invariant sets are trivial, in other words if $\mu(T^{-1}E \triangle E) = 0$ implies that $\mu(E) = 0$ or 1, where $\triangle$ is the symmetric difference.

Given two open covers $\mathcal{A}, \mathcal{B}$ of the compact topological space X, define their *join* to be $\mathcal{A} \vee \mathcal{B} = \{A \cap B : A \in \mathcal{A},\ B \in \mathcal{B}\}$, and define the entropy of $\mathcal{A}$ to be $H(\mathcal{A}) = \log N(\mathcal{A})$ where $N(\mathcal{A})$ is the number of sets in a finite subcover with minimal cardinality. The *topological entropy* of a continuous map $T : X \to X$ is defined to be

$$h(T) = \sup_{\mathcal{A}} \lim_{n\to\infty} \frac{1}{n} H\Big(\bigvee_{j=0}^{n-1} T^{-j}(\mathcal{A})\Big),$$

where the supremum is taken over all open covers of X (see [1]; the topological entropy is a measure of orbit complexity introduced as an analogue of the measure-theoretic entropy).

The β-transformation T_β is defined for real $\beta > 0$ on the interval $[0, 1)$ by $T_\beta(x) = \{\beta x\} = \beta x \pmod 1$. If $\beta > 1$, the β-transformation preserves an absolutely continuous probability measure with respect to which it is ergodic [13], the (measure-theoretic and topological) entropy is $h(T_\beta) =$

$\log\beta$ (see [11] and [12], [9]) and (see [7]) the asymptotic growth rate of the periodic points equals the entropy. The result about the asymptotic growth rate will be applied in Section 5 (see (13)). Strictly speaking, the definition of topological entropy in terms of open covers does not apply to the classical β-transformation because it has a discontinuity; the topological entropy referred to is that of an associated shift system (see [21, Sec. 7.3]). If $\beta \le 1$, the map is simply multiplication by β. If $\beta < 1$, T_β does not preserve an absolutely continuous measure, it has topological entropy zero and has no periodic points apart from 0. In all cases, the entropy is $h(T_\beta) = \log^+\beta$.

Now we define a p-adic analogue of the β-transformation. For any $q \in \mathbb{Q}_p$, define a map, denoted by T_q, sometimes referred to as the q-transformation, as follows. Let x be a generic element of $\mathbb{Z}_p$ and write $qx = \sum_{i=m}^{\infty} b_i p^i$. Define

$$T_q(x) = \sum_{i=\max\{0,m\}}^{\infty} b_i p^i.$$

In other words, T_q multiplies by q and cuts away the fractional tail in order to come back to $\mathbb{Z}_p$. Note that T_q could be defined over $p\mathbb{Z}_p$ in an analogous way, and the ergodic properties would not change once the Haar measure had been normalized again.

1. If $|q|_p \ge 1$, the map T_q preserves Haar measure on $\mathbb{Z}_p$.

2. If $|q|_p < 1$ then T_q is multiplication by q, and it only preserves the point mass at the identity.

3. The ring of p-adic integers $\mathbb{Z}_p$ is homeomorphic to the space $X = \prod_{n\in\mathbb{N}} Y$ of one-sided sequences with elements in $Y = \{0, \dots, p-1\}$, and $T_{1/p}$ is conjugate to the left shift σ on X.

THEOREM 4.1. *The topological entropy of the p-adic q-transformation is given by $h(T_q) = \log^+ |q|_p$.*

P r o o f. We follow Bowen [2] and compute the topological entropy as a volume growth rate. It is a straightforward computation to check that Haar measure on $\mathbb{Z}_p$ is T_q-homogeneous, so (see [2, Prop. 7])

$$h(T_q) = \lim_{m\to\infty} \limsup_{n\to\infty} -\frac{1}{n} \log \mu\Big(\bigcap_{k=0}^{n-1} T_q^{-k} B_m \Big) \tag{8}$$

where $B_m = p^m\mathbb{Z}_p$.

If $|q|_p \le 1$, then $T_q^{-1}B_m \supset B_m$ so

$$\bigcap_{k=0}^{n-1} T_q^{-k} B_m = B_m,$$

and (8) gives $h(T_q) = 0 = \log^+ |q|_p$.

If $|q|_p = p^r > 1$, then $T_q^{-1} B_m = B_{m+r}$, so

$$\bigcap_{k=0}^{n-1} T_q^{-k} B_m = B_{m+rn},$$

so by (8) we have $h(T_q) = r \log p = \log^+ |q|_p$. ∎

THEOREM 4.2. *Let $q \in \mathbb{Q}_p$ with $|q|_p \geq 1$. The map T_q is ergodic with respect to Haar measure for $|q|_p > 1$, and is not ergodic for $|q|_p = 1$.*

Proof. When q is a unit, the open sets of the form $p^n \mathbb{Z}_p$ for $n \geq 1$ are all invariant under T_q, so the map is not ergodic.

If $|q|_p > 1$ then it is clear the map is ergodic, since it behaves as a group rotation followed by a full shift. ∎

A consequence of properties 1, 2 for the systems in Section 1 is that the logarithmic growth rate of the periodic points, $\lim_{n\to\infty}(1/n) \log \mathrm{Per}_n(T_F)$, coincides with the entropy (see [6, Lemma 1.10]). That this also holds for T_q follows from the next result.

THEOREM 4.3. *Given $q \in \mathbb{Q}_p \setminus U$, where U denotes the set of unit roots in $\mathbb{Q}_p$, let T_q denote the q-transformation on $\mathbb{Z}_p$. Then*

$$\log |\mathrm{Per}_n(T_q)| = n \log^+ |q|_p. \tag{9}$$

Proof. First, consider the case $|q|_p < 1$. Then as $n \to \infty$ we have $T_q^n(x) \to 0$ for all $x \in \mathbb{Z}_p$. Thus T_q has only one periodic point (zero) and both sides of (9) are zero.

When $|q| = 1$, the action of q on $\mathbb{Z}_p$ is simply multiplication, so the periodic points are solutions to the equation $q^n x = x$. Since q is not a unit root, there are no periodic points except $x = 0$, so (9) holds.

Finally, suppose $|q|_p > 1$. If $q = p^{-k}$ with $k > 0$, the periodic points are easy to determine. We have $T_q^n(x) = \sum_{i=0}^{\infty} a_{i+nk} p^i$ and the solutions to $T_q^n x = x$ are given by the p^{kn} points with $a_{i+nk} = a_i$ for $i = 0, \ldots, kn-1$. Thus, both sides of (9) are equal to $nk \log p$. In general, suppose $|q|_p = p^k$. We claim that for each integer a with $0 \leq a < p^{nk}$, there is a unique $y \in \mathbb{Z}_p$ with $T_q^n(a + p^{nk} y) = a + p^{nk} y$. This follows because the left hand side is $b + q^n p^{nk} y$ for some $b \in \mathbb{Z}_p$, which depends only upon a, q and n. Write $q^n p^{nk} = v$ for some p-adic unit v then the equation $b + vy = a + p^{nk} y$ has a unique solution for $y \in \mathbb{Z}_p$. This shows that there are at least p^{nk} solutions of $T_q^n x = x$. That there can be no more follows because we may take the a as above as coset representatives for $\mathbb{Z}_p / p^{nk} \mathbb{Z}_p$ so every element $x \in \mathbb{Z}_p$ is represented by some a. ∎

In conclusion, given any p-adic elliptic curve E and any point $Q \in E(\mathbb{Q}_p)$, we can construct a dynamical system in the following way. The curve is

locally isomorphic to the group $p\mathbb{Z}_p$ and therefore to $\mathbb{Z}_p$. Now let Q act via the q-transformation on the additive curve, where $q = x(Q)$. Then transport this action to the curve proper via the logarithm. This is an exact analogue of the toral dynamical systems in Sections 1 and 2.

5. Dynamics on the elliptic adeles. From here on, let E denote an elliptic curve defined over $\mathbb{Q}$ and let $Q \in E(\mathbb{Q})$. The explicit formula (6) for the local height of Q does not hold if Q has bad reduction or if p is the prime at infinity. In particular, the local height in these cases can be negative. Since the entropy of a map is never negative, we will work with points whose local heights are guaranteed to be non-negative.

CLAIM 5.1. *There exists an $n \geq 1$ for which $\lambda_p(Q) \geq 0$ for all $p < \infty$ and $Q \in nE(\mathbb{Q})$.*

Proof. Since $E_1(\mathbb{Q}_p)$ is a subgroup of finite index in $E(\mathbb{Q}_p)$ (simply by noting that $E_1(\mathbb{Q}_p)$ is the kernel of the reduction mod p map, which has finite image), for each bad prime p there exists an integer n_p such that $E_1(\mathbb{Q}_p)$ has index n_p in $E(\mathbb{Q}_p)$. Let $n = \prod_{\text{bad } p} n_p$; then $nE(\mathbb{Q}_p) \leq E_1(\mathbb{Q}_p)$ for all bad p. Points in $E_1(\mathbb{Q}_p)$ have $\lambda_p \geq 0$ by (6) since such a point has good reduction by construction. Recall now that if Q has good reduction at p then the local height at p is again given by (6) and it follows that $\lambda_p(Q) \geq 0$. ∎

Define $\mathcal{S}$ to be the set of bad primes together with infinity. Assume that the point Q satisfies

$$\lambda_p(Q) > 0 \quad \text{for all } p \in \mathcal{S}. \tag{10}$$

If $Q \in nE(\mathbb{Q})$ then $Q \in E_1(\mathbb{Q}_p)$ for each bad prime p. It follows from (6) that the local height is actually positive. If the rank of $E(\mathbb{Q})$ is not zero then $nE(\mathbb{Q})$ has finite index in $E(\mathbb{Q})$ so in that case, there is a large stock of points Q which satisfy (10). At the infinite prime, this amounts to assuming that Q lies in a neighbourhood of the identity by the explicit form in [16, Sec. 18].

Suppose $Q \in E(\mathbb{Q})$ is a point for which the assumption (10) holds. Define X to be the space

$$X = \prod_{p \leq \infty} E_1(\mathbb{Q}_p). \tag{11}$$

The point Q induces an action $T_Q : X \to X$ in the following way: $(T_Q)_p$ is the q-transformation if p is finite (where $q = a/b = x(Q)$) and the β-transformation if p is infinite, where $\log \beta = 2\lambda_\infty(Q)$. These are actions on $\mathbb{T}$ and $p\mathbb{Z}_p$, but for every p, the action can be transported to $E_1(\mathbb{Q}_p)$ via the isomorphisms in Section 3. The statements in the following theorem are

analogues of statements 1 and 2 in the introduction. There we supposed that the zeros of F were not torsion points of $\mathbb{T}$. The assumption that Q is not a torsion point of E is built into (10): Q is a torsion point if and only if $\widehat{h}(Q) = 0$ and (10) guarantees that $\widehat{h}(Q) > 0$.

THEOREM 5.2. *With the definitions and assumptions above, and* $q = a/b = x(Q)$,

1. *the entropy of* T_Q *is given by* $h(T_Q) = 2\widehat{h}(Q)$, *and*
2. *the asymptotic growth rate of the periodic points is given by the division polynomial* $\nu_n(x)$ *in* (7):

$$\log|\mathrm{Per}_n(T_Q)| \sim \log|b^n\nu_n(q)| \quad \text{as } n \to \infty.$$

Proof. By Theorem 4.1, the entropy of each component of T_Q is given by $\log\beta_p$, where $\beta_p = \beta$ if $p = \infty$ and $\beta_p = \max\{|x(Q)|_p, 1\}$ if p is finite. Since there are only finitely many primes for which the local dynamical systems are not isometries, Theorem 4.23 in [21] applies giving

$$h(T_Q) = h(T_\beta) + \sum_{p<\infty} h(T_q) = \sum_{p\le\infty} \log\beta_p = 2\sum_p \lambda_p(Q) = 2\widehat{h}(Q).$$

For the asymptotic growth rate of the periodic points note that if dynamical systems $\widehat{T}_i : X_i \to X_i$ $(i = 1, \dots, r)$ are given and the point x_i has period m under $\widehat{T}_i$ for $i = 1, \dots, r$ then (x_i) has period m under $\prod_i \widehat{T}_i$. Thus we may count the contribution to the periodic points from each prime separately. For $p < \infty$, from Theorem 4.3,

$$\log|\mathrm{Per}_n(T_q)| = n\log^+|q|_p = -n\log|b|_p. \tag{12}$$

Note that our assumption on Q guarantees that q is not an integer and so, in particular, q is not a root of unity. Summing over all finite p and using the product formula, we obtain a total contribution of $n\log|b|$ to the periodic points. For the infinite prime, we quote a deep result from [7] which says

$$\log|\mathrm{Per}_n(T_\beta)| = n\log\beta + o(n). \tag{13}$$

From (11) and (12) we have the formula

$$\log|\mathrm{Per}_n(T_Q)| = n\log|b| + n\log\beta + o(n). \tag{14}$$

Finally, we quote from Theorem 6.24 in [6] which gives

$$\log|\nu_n(q)| = n\log\beta + o(n). \tag{15}$$

The formula (15) depends upon an application of the elliptic analogue of Baker's theorem from transcendence theory (see [4], [5, Sec. 7] and [6, Th. 6.18]). It follows from (14) and (15) that $\log|b^n\nu_n(q)|$ is asymptotically equivalent to $\log|\mathrm{Per}_n(T_Q)|$. ∎

Set now $\mathcal{S}^*(Q) = \{p : |x(Q)|_p > 1\} \cup \{\infty\}$, let $X^* = \prod_{p\in\mathcal{S}^*(Q)}$ and let T_Q^* be defined component-wise as above.

THEOREM 5.3. 1. *The entropy of T_Q^* is given by $h(T_Q^*) = 2\widehat{h}(Q)$.*

2. *The asymptotic growth rate of the periodic points is given by the division polynomial* (7):

$$\log|\mathrm{Per}_n(T_Q^*)| \sim \log|b^n\nu_n(q)|.$$

3. *T_Q^* is ergodic.*

P r o o f. For the entropy and the periodic points, the same argument as in Theorem 5.2 holds giving the desired result. The ergodicity is proved in Theorem 4.2. ∎

The pros and cons of our construction may be summarized as follows. Firstly, we have constructed a dynamical system whose immanent group is the adelic elliptic curve. The map is defined locally by the p-adic β-transformation on the additive curve. Secondly, the construction exhibits phenomena which resemble those in the solenoid case. Against these comments we must set the following. Firstly, the maps we are using are not continuous because of the discontinuity of the classical β-transformation. The effect upon the map T_Q is to deny continuity at infinity on the archimedean component. Secondly, we would have preferred to see periodic point behaviour which was counted precisely by the usual elliptic division polynomial (rather than just asymptotically by the real division polynomial). Thirdly, the map at the archimedean prime uses *a priori* knowledge of the archimedean height of the point. Fourthly, we made special assumptions to guarantee that each local height was non-negative. Although these assumptions were natural, at the infinite prime and each bad prime we assumed our point was to be found in a neighbourhood of the identity, we would have preferred not to have needed any assumptions. In the next section, we discuss how these deficiencies might be overcome.

6. Putative elliptic dynamics. Suppose E denotes an elliptic curve defined by a generalized Weierstrass equation with integral coefficients. For each $n \in \mathbb{N}$, let $\psi_n(x) = n^2x^{n^2-1} + \dots$ denote the nth division polynomial. Let Q denote a non-torsion rational point on E, with $x(Q)=a/b$. It is tempting to conjecture that there is a compact space X with a continuous action $T_Q : X \to X$ whose entropy is given by $h(T_Q) = 2\widehat{h}(Q)$, and whose periodic points are counted, in the sense of Section 1, by $E_n(Q)=|b^{n^2-1}\psi_n(a/b)|$. It is known (see [6, Ex. 6.12]) that $E_n(\mathbb{Q})$ is given by the determinant of a Hankel matrix. This is analogous to the way that the periodic points formula for the toral case (2) arises as the determinant of a circulant matrix. However, there is a problem in making the obvious conjecture. When E is given by the

equation $y^2+y=x^3-x$ and Q is the point $Q=(0,0)$, the sequence begins $1,1,1,1,2,\ldots$ which cannot be the sequence of periodic points for any bijection (since the first and fifth term are not congruent modulo 5, for example). Of course, this does not preclude the possibility that there is a non-invertible map with exactly these data. In addition, the quadratic-exponential growth rate characteristic to elliptic curves is not usually seen in the dynamics of iterates of single transformations. Such rates do however naturally occur for $\mathbb{Z}^2$-actions, but we are not able to pursue this at the moment.

We believe that the appearance of the canonical height as an entropy might well provide an interesting interpretation for the "shape" of the height as a sum of local heights. We know that the local heights can be negative so the global height is usually the difference of two positive contributions. Although a negative entropy cannot exist, nonetheless, the difference between two non-negative entropies can make sense. If one dynamical system extends another then the difference between their two entropies represents the entropy on the fibres. This raises the possibility that a phenomenon such as bad reduction might well have a dynamical interpretation.

Interest in our conjecture (see [6, Question 14]) is heightened because of the connection with the following remarkable circle of ideas. On the one hand, mathematical physicists have studied the dynamics of integrable systems (see [19], [20]). Here, *inter alia*, one looks for meromorphic maps on the complex plane which commute with polynomials. It is a classical result of Ritt (see [14]) that all non-trivial examples arise from the exponential function or the elliptic functions associated with some lattice. Coincidentally, Morgan Ward (see [22], [23]) showed that all integer sequences satisfying a certain natural recurrence relation arise from the exponential function or the elliptic functions associated with some lattice, suitably evaluated. In the exponential case, these sequences play a fundamental role in describing the dynamics of toral systems. It is hoped that in the elliptic case also, the sequences $|\psi_n(a)|$ play a fundamental role in describing the dynamics of some elliptic systems. That being so, a new chapter in integrable systems could be written, yielding further interplay between elliptic curves and mathematical physics.

REFERENCES

[1] R. Adler, A. Konheim and M. McAndrew, *Topological entropy*, Trans. Amer. Math. Soc. 114 (1965), 309–319.

[2] R. Bowen, *Entropy for group endomorphisms and homogeneous spaces*, ibid. 153 (1971), 401–414.

[3] V. Chothi, G. Everest and T. Ward, *S-integer dynamical systems: periodic points*, J. Reine Angew. Math. 489 (1997), 99–132.

[4] S. David, *Minorations des formes linéaires de logarithmes elliptiques*, Mem. Soc. Math. France 62 (1995).
[5] G. Everest and T. Ward, *A dynamical interpretation of the global canonical height on an elliptic curve*, Experiment. Math. 7 (1998), 305–316.
[6] —, —, *Heights of Polynomials and Entropy in Algebraic Dynamics*, Springer, London, 1999.
[7] L. Flatto, J. C. Lagarias and B. Poonen, *The zeta function of the beta transformation*, Ergodic Theory Dynam. Systems 14 (1994), 237–266.
[8] E. Hewitt and K. Ross, *Abstract Harmonic Analysis*, Springer, New York, 1963.
[9] F. Hofbauer, *β-shifts have unique maximal measures*, Monatsh. Math. 85 (1978), 189–198.
[10] D. A. Lind and T. Ward, *Automorphisms of solenoids and p-adic entropy*, Ergodic Theory Dynam. Systems 8 (1988), 411–419.
[11] W. Parry, *On the β-expansions of real numbers*, Acta Math. Acad. Sci. Hungar. 11 (1960), 401–416.
[12] —, *Representations for real numbers*, ibid. 15 (1964), 95–105.
[13] A. Rényi, *Representations for real numbers and their ergodic properties*, ibid. 8 (1957), 477–493.
[14] J. F. Ritt, *Permutable rational functions*, Trans. Amer. Math. Soc. 25 (1923), 399–448.
[15] K. Schmidt, *Dynamical Systems of Algebraic Origin*, Birkhäuser, Basel, 1995.
[16] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, New York, 1986.
[17] —, *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358.
[18] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York, 1994.
[19] A. P. Veselov, *What is an integrable mapping?*, in: What is Integrability?, V. E. Zakharov (ed.), Springer, New York, 1991, 251–272.
[20] —, *Growth and integrability in the dynamics of mappings*, Comm. Math. Phys. 145 (1992), 181–193.
[21] P. Walters, *An Introduction to Ergodic Theory*, Springer, New York, 1982.
[22] M. Ward, *The law of repetition of primes in an elliptic divisibility sequence*, Duke Math. J. 15 (1948), 941–946.
[23] —, *Memoir on elliptic divisibility sequences*, Amer. J. Math. 70 (1948), 31–74.
[24] T. Ward, *The entropy of automorphisms of solenoidal groups*, Master's thesis, Univ. of Warwick, 1986.
[25] A. Weil, *Basic Number Theory*, third ed., Springer, New York, 1974.

School of Mathematics
University of East Anglia
Norwich NR4 7TJ, UK
E-mail: g.everest@uea.ac.uk
t.ward@uea.ac.uk

Received 21 May 1999;
revised 16 November 1999 (3763)